Lernauftrag
Die Windows Registry

Version	1.0
Datum	08.05.2016
Anzahl Seiten	

Änderungshistorie

Version	Datum	Änderungen
1.0	08.05.16	Initiale Erstellung

Vorbemerkungen

Immer wieder stelle ich in meinem Arbeitsalltag fest, dass **selbst langjährige IT Mitarbeiter nur wenige Erfahrungen mit der Windows Registrierungsdatenbank (englische Kurzform: Registry) besitzen** und entsprechend Probleme damit haben, diese zur Fehlerbehebung oder Konfiguration von Systemen zu verwenden.

Gerade deshalb finde ich es **vor Allem auch für Auszubildende bzw. Umschüler besonders wichtig**, sich mit diesem **zentralen Teil der Windows-Betriebssystemkonfiguration eingehender zu beschäftigen**.

Dieser geführte Lernauftrag konzentriert sich hauptsächlich auf die Aspekte, mit denen man, wie ich aufgrund meiner bisherigen Berufserfahrung als IT-Administrator feststellen konnte, Im Arbeitsalltag am häufigsten in Berührung kommt. Dieses Dokument erhebt daher keinen Anspruch auf Vollständigkeit oder uneingeschränkte Richtigkeit, es soll lediglich als geführter Lernauftrag für das Selbststudium des Themas dienen.

Die Tools welche ich vorstelle sind Werkzeuge die ich persönlich verwende und daher empfehlen möchte und kann.

Zudem sind die genannten Einstellungen, Tools, Konfigurationen oder Hinweise persönliche Empfehlungen, welche ebenfalls weder allgemein gültig noch richtig sein müssen.

DISCLAIMER: Jegliche Änderungen an der Windows Registrierung sowie alle Änderungen an Programmeinstellungen nehmen Sie auf eigene Gefahr vor. Durch den unsachgemäßen Umgang bzw. durch fehlerhafte Einstellungen kann es zu Instabilitäten der Programme oder des Betriebssystems kommen.

Was ist die Windows Registry?

Sowohl Microsoft selbst als auch zum Beispiel Wikipedia erklären die Windows Registrierungsdatenbank (meist nur Registrierung oder mit dem gebräuchlichen englischen Begriff Registry abgekürzt) als eine hierarchische Datenbank welche unter anderem Informationen zu

- installierter Soft- und Hardware
- Konfigurationseinstellungen von Windows und installierten Programmen
- Dateitypen und deren zugehörigen Standardanwendungen
- Benutzerprofilen und deren individuelle Einstellungen

enthält.

Historisch betrachtet wurden mit dieser zentralen Datenbank die unzähligen separaten Konfigurationsdateien (z.Bsp. *.ini, *.sys oder *.com), welche bis Windows 3.1 verwendet wurden, abgelöst.

Dies bietet verschiedene Vorteile:

1.) Mit Hilfe des Registrierungs-Editors ist es möglich, **zentral alle Einstellungen einzusehen und zu bearbeiten**, anstatt unzählige Konfigurationsdateien zu durchsuchen. Auch unnötige Redundanzen lassen sich somit vermeiden.

2.) **Programme** können über eine **Standardschnittstelle Werte** aus der Registrierung **auslesen, einfügen, bearbeiten oder gar löschen** (sofern der entsprechende Benutzer das Recht dazu hat).

3.) **Berechtigungen** können **granularer** als nur auf Datei-Ebene (auf Schlüssel-Ebene) vergeben werden.

4.) Mit Hilfe von **Gruppenrichtlinien** können in einer **Active Directory Domäne** über eine grafische Oberfläche identische **Registrywerte auf die gewünschten Windows-Endgeräte verteilt werden**.

Allgemeiner Aufbau

Auch wenn die bisherigen Ausführungen durchaus die Vermutung zulassen, dass es sich bei der Registry um eine einzige Datei handelt, stimmt dies leider nicht. Viel mehr werden in der Registry die Informationen aus unterschiedlichen einzelnen Teilstrukturen zusammengeführt die auf der einen Seite system- / computerspezifische Informationen widerspiegeln und auf der anderen Seite benutzerspezifische Einstellungen zeigen.

Schauen wir uns die Registry doch einmal an.

Die obige **Grafik zeigt 5 Teilstrukturen**, welche alle mit HKEY beginnen. Dies steht für **Hive Keys** zu deutsch Bienenstock-Schlüssel.

Tatsächlich existieren jedoch nur 2 Teilstrukturen, nämlich:

HKEY_USERS (benutzerspezifische Einstellungen)
und
HKEY_LOCAL_MACHINE (computerspezifische Einstellungen)

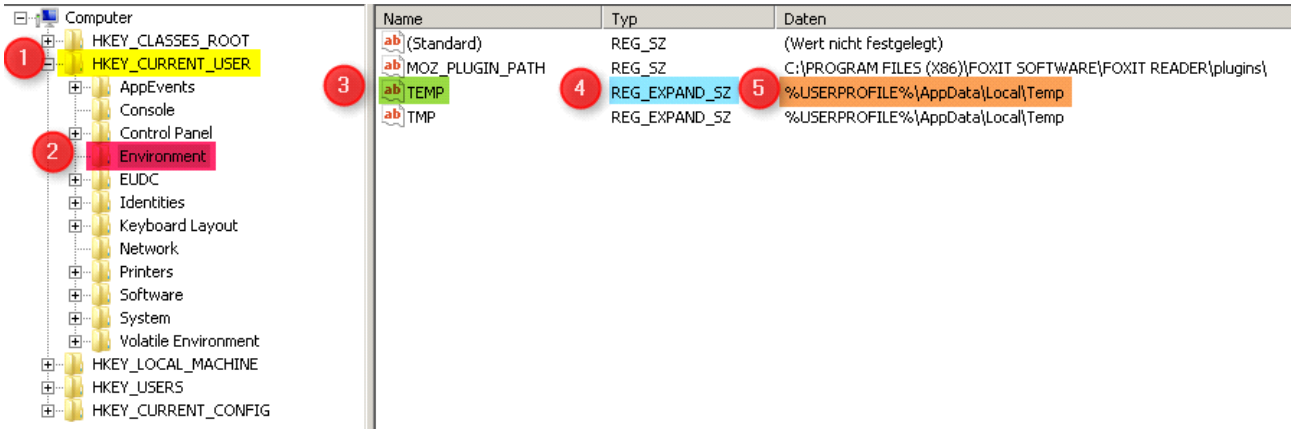
Die anderen drei Teilstrukturen dienen nur als eine Art „Alias“ bzw. Verweis auf bestimmte Unterstrukturen von HKEY_USERS bzw. HKEY_LOCAL_MACHINE.

Eine etwas ausführlichere Darstellung findet sich im folgenden Microsoft Technet Artikel:
https://technet.microsoft.com/de-de/library/cc776231

Ich gehe auf jeden dieser 5 Teilschlüssel noch einmal nachstehend in einer etwas ausführlicheren Aufbereitung ein.

Begriffe und Datentypen

Bevor wir uns die einzelnen Hive-Keys jedoch anschauen, möchte ich noch die Begrifflichkeiten rund um die Registry klären sowie die verschiedenen Datentypen vorstellen die man finden kann.



1.) Hive

Die Hives sind die 5 Hauptschlüssel die im vorhergehenden Kapitel zu sehen waren.
In der Beispielgrafik befinden wir uns im **Hive HKEY_CURRENT_USER**

2.) Schlüssel (bzw. Unterschlüssel)

So werden alle Unterstrukturen genannt, welche keine Werte und Wertdaten darstellen. Sie dienen zur Strukturierung der Registrierung.
In der Beispielgrafik lautet die Bezeichnung des **Schlüssels ENVIRONMENT**

3.) Wert

Der Wert steht für einen bestimmten Konfigurationswert.
In der Beispielgrafik lautet der **Wert***name* **TEMP**

4.) Werttyp

Jeder Wert ist von einem bestimmten Typ (eine Übersicht folgt in der nachstehenden Grafik) welche sich je nach Inhalt unterscheiden.
In der Beispielgrafik ist der **Typ des Wertes REG_EXPAND_SZ**

5.) Wertdaten

Die Wertdaten sind letztendlich die Informationen die der Wert enthält bzw. darstellt.
In der Beispielgrafik sind die **Daten** *die erweiterbare Zeichenfolge* **%USERPROFILE%\AppData\Local\Temp**

In der folgenden Tabelle sind die unterschiedlichen Werttypen benannt und welche Daten sie üblicherweise enthalten bzw. für welche Werte sie häufig gebräuchlich sind.

Typ	Name	Beschreibung
REG_SZ	Zeichenkette (engl. String)	Einfache Zeichenketten aus Unicode-Zeichen welche Text oder Zahlenwerte enthalten und immer von Anführungszeichen eingeschlossen sein müssen
REG_MULTI_SZ	Wert der mehrteiligen Zeichenfolge (Multistring)	Mehrteilige Zeichenfolgen enthalten mehrere Werte oder Listen in lesbarem Format. Die einzelnen Einträge werden durch Trennzeichen voneinander abgegrenzt.
REG_EXPAND_SZ	Wert der erweiterbaren Zeichenfolge (Expandable String)	Eine erweiterbare Zeichenfolge beinhaltet eine Variable die zur Laufzeit in die entsprechende Zeichenfolge aufgelöst wird.
REG_BINARY	Binärwert (Binary)	Binärcode welcher direkt verarbeitet werden kann. Dieser wird im Hexadezimalformat angezeigt.
REG_DWORD	DWORD-Wert (32-Bit) (DWORD (32-Bit)	Daten die mittels einer 4Byte (32 Bit) großen Integer-Zahl dargestellt werden. Diese können im Dezimal, Hexadezimal oder Binärformat vorkommen.
REG_QWORD	QWORD-Wert (64-Bit) (QWORD (32-Bit)	Daten die mittels einer 8Byte (64 Bit) großen Integer-Zahl dargestellt werden.Ansonsten identisch mit dem REG_DWORD.

HKEY_CLASSES_ROOT

Im **alphabetisch an erster Stelle stehenden Teilschlüssel vereinen** sich sowohl die **computer- als auch benutzerspezifischen Informationen** zu bekannten **Dateitypen**, mit **welchen Programmen diese zu öffnen bzw. zu bearbeiten sind**, die ProgIDs (identifiziert Programmklassen, aber weniger genau), CLSIDs (identifiziert eindeutig ein COM-Klassenobjekt) und IIDs (identifiziert eindeutige Schnittstellen).

Der **Hauptzweck dieses Teilschlüssels** besteht in der **(Rückwärts-)Kompatibilität zu früheren Windows Versionen** und Programmen, welche den damaligen Registrierungsaufbau weiterhin annehmen.

Damals gab es keinen benutzerspezifischen Teil. Dieser wurde unter dem Begriff „**Per-User Class Registration**“ eingeführt und bietet folgende Vorteile:

- Verschiedene Benutzer können unterschiedliche Applikationen installieren, welche zum Darstellen oder Bearbeiten eines bestimmten Dateityps gedacht sind, ohne dass die Einstellungen der anderen Benutzers verändert oder beeinträchtigt werden.

- Da früher die Änderung des Standardprogramms systemweit übernommen wurde, kam es durchaus vor, dass ein Benutzer der ein falsches oder abweichendes Standardprogramm definierte, nicht nur seine Zuordnung zerstörte, sondern auch die aller anderen Benutzer des Systems.

Deshalb werden unter diesem Teilschlüssel nun folgende beide Teilstrukturen

HKEY_LOCAL_MACHINE\SOFTWARE\Classes (gilt systemweit)
HKEY_CURRENT_USER\SOFTWARE\Classes (gilt nur für den angemeldeten Benutzer)

nach folgenden Regeln zusammengeführt dargestellt:

1.) **Ein Wert wird unter HKEY_CLASSES_ROOT angezeigt, wenn er in einem der oben genannten Teilschlüssel vorhanden ist**.

2.) Ist ein **Wert in beiden Teilschlüsseln vorhanden, wird immer der Wert aus HKEY_CURRENT_USER\SOFTWARE\Classes angezeigt und besitzt auch innerhalb der Benutzersitzung Vorrang vor den Standardwerten aus HKEY_LOCAL_MACHINE.**

ERGO: Dieser Teilschlüssel kann auf dem gleichen PC / Server unterschiedliche Werte beinhalten, je nachdem welcher Benutzer angemeldet ist.

Dies erklärt auch folgende Microsoft-Empfehlungen:

1.) Soll eine **Änderung nur für den interaktiven** (sprich: angemeldeten) **Benutzer** vorgenommen werden, so sollen die Änderungen **im Schlüssel HKEY_CURRENT_USER\SOFTWARE\Classes** vorgenommen werden und **nicht unter HKEY_CLASSES_ROOT**.

2.) Um die Standardeinstellung **für das gesamte System anzupassen**, sollen die Änderungen **im Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Classes**

vorgenommen werden und **nicht unter HKEY_CLASSES_ROOT**.

Eine Änderung der Werte unter HKEY_CLASSES_ROOT kann in verschiedenen Fällen nicht zu dem gewünschten Ergebnis führen, da

1.) Wenn ein **neuer Schlüssel oder Unterschlüssel unter HKEY_CLASSES_ROOT erstellt** wird, wird **somit ein neuer Schlüssel bzw. Unterschlüssel unter HKEY_LOCAL_MACHINE\SOFTWARE\Classes** erstellt.

2.) Wird ein **neuer Wert unter einem bestehenden Schlüssel oder Unterschlüssel** von **HKEY_CLASSES_ROOT** erzeugt, wird der **neue Wert in der Teilstruktur abgelegt**, in welcher sich der **Schlüssel oder Unterschlüssel bereits befand** und gilt somit **entweder nur für den aktuellen Benutzer oder systemweit**.

3.) **besteht der Schlüssel bzw. Unterschlüssel in beiden Strukturen**, wird der n**eue Wert NUR unter HKEY_CURRENT_USER\SOFTWARE\Classes** erzeugt

4.) besteht der Schlüssel bzw. Unterschlüssel nur in **HKEY_CURRENT_USER\ SOFTWARE\Classes** wird der neue Wert auch nur dort angelegt.

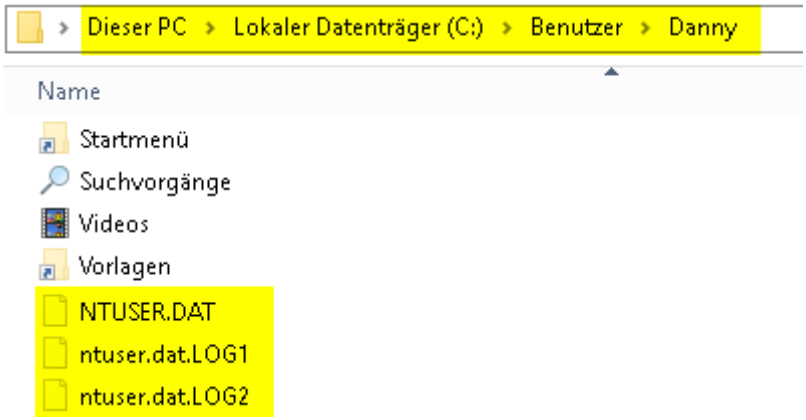
5.) besteht der Schlüssel bzw. Unterschlüssel nur in **HKEY_LOCAL_MACHINE\ SOFTWARE\Classes** wird der neue Wert auch nur dort angelegt.

HKEY_CURRENT_USER

In der alphabetisch nächstsortierten Teilstruktur HKEY_CURRENT_USER finden sich die benutzerspezifischen Einstellungen des interaktiven (aktuell angemeldeten Benutzers).

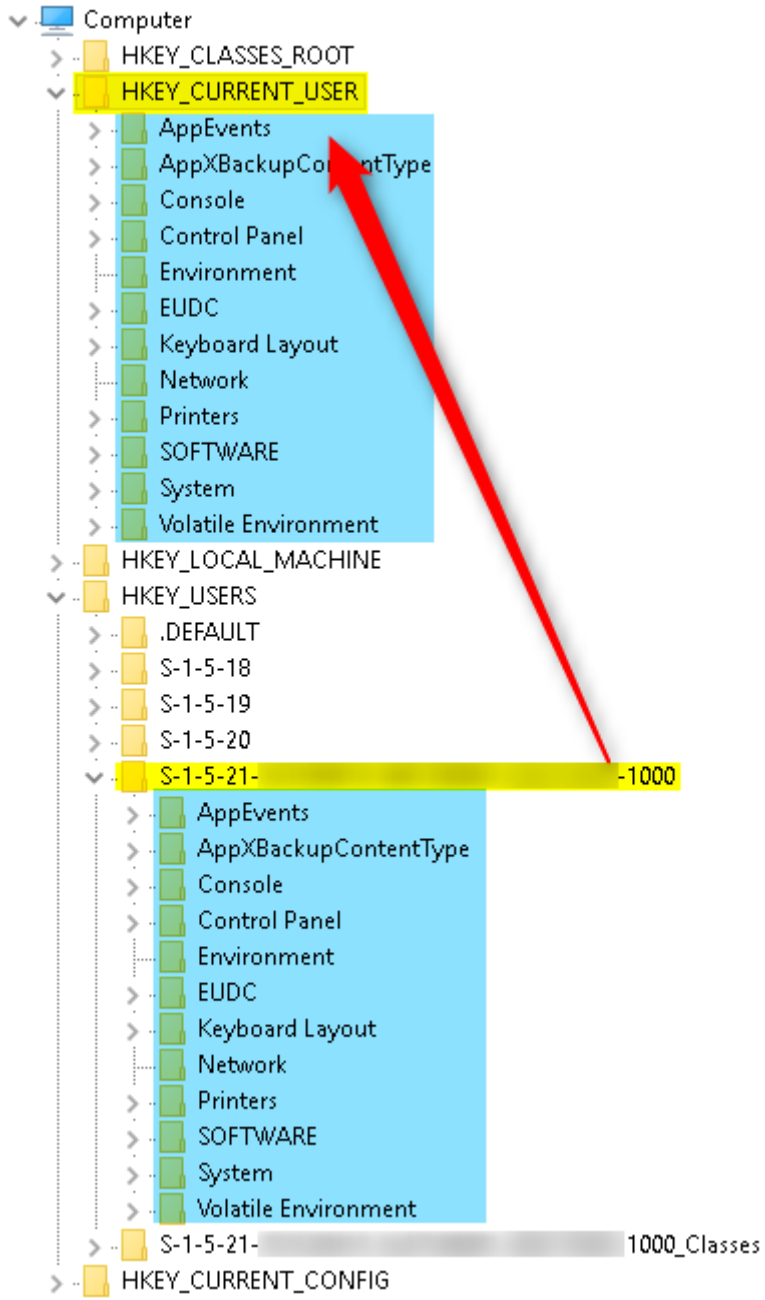
Diese spiegeln die Einstellung des Benutzer-Unterordners des Zweiges HKEY_USERS wieder.

Die Einstellungen sind in der **Datei ntuser.dat in jedem Benutzerprofil gespeichert**.
Zu dieser Datei gibt es jeweils entsprechend auch Logfiles.

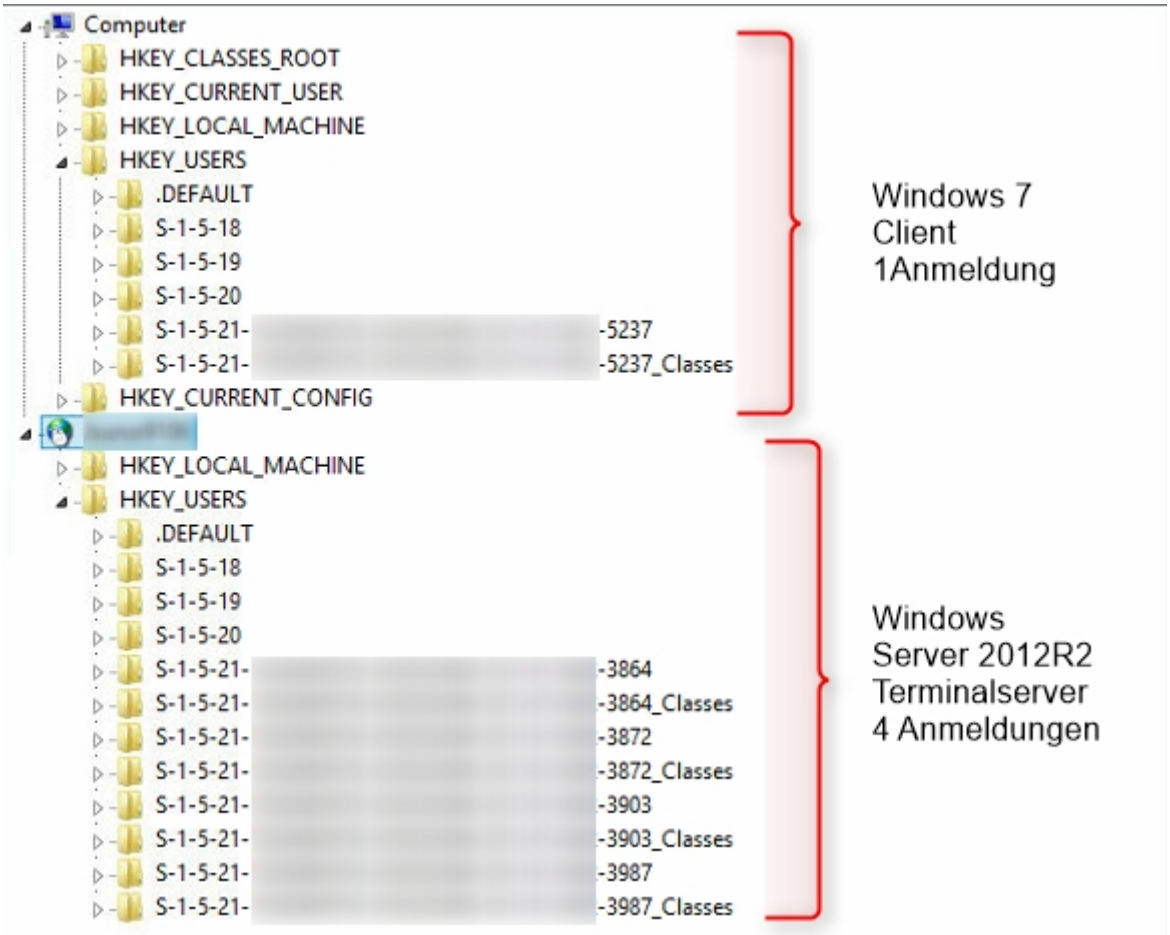


Diese Datei wird bei der Benutzeranmeldung an einem Windows-System in der Registrierungsdatenbank mit der SID des Benutzers als Bezeichner in der Teilstruktur HKEY_USERS “eingehangen”.

Dieser Zweig enthält benutzerspezifische Softwareeinstellungen, die Umgebungsvariablen des Benutzers, die Einstellungen des Desktops, Druckereinstellungen, etc.



Sind also parallel mehrere Benutzer an einem Windows System angemeldet, finden sich in der Struktur “HKEY_USERS” mehr “Unterschlüssel” (zum Beispiel auf einem Terminalserver) als wenn nur ein Benutzer an dem System angemeldet ist.



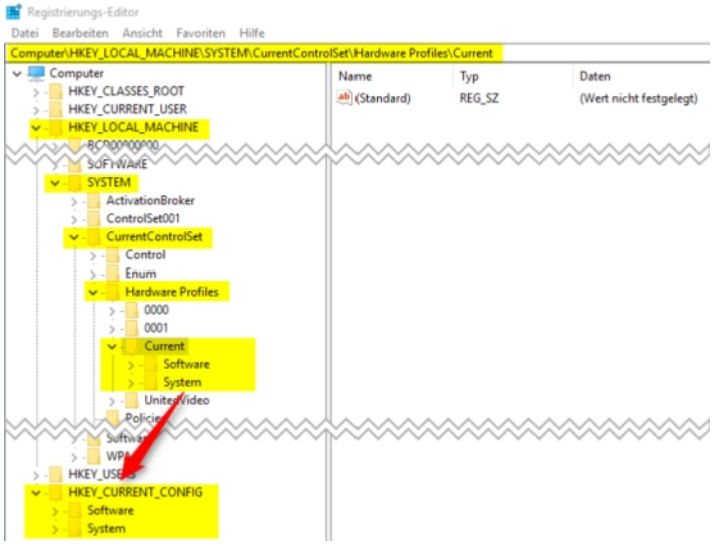
HKEY_CURRENT_CONFIG

In der Teilstruktur HKEY_CURRENT_Config finden sich Informationen zu der aktuellen Hardware-Konfiguration.

Die hier dargestellten Einstellungen spiegeln die Werte aus dem Zweig

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\HardwareProfile\Current

wieder.



In diesem Zweig werden nur die Unterschiede zu der Standard Hardwarekonfiguration des Systems gespeichert.

Die Standardkonfiguration ergibt sich aus den beiden HKLM-Schlüsseln
Software
System

Das Ändern bzw. Auslesen von Wertdaten aus diesem Teil der Registry habe ich bisher in meinem Itler-Dasein noch nicht bewusst benötigt.

HKEY_LOCAL_MACHINE

Dieser Hive umfasst alle computerspezifischen Konfigurationseinstellungen der Windows Registrierungsdatenbank und wird häufig schlicht mit HKLM abgekürzt.

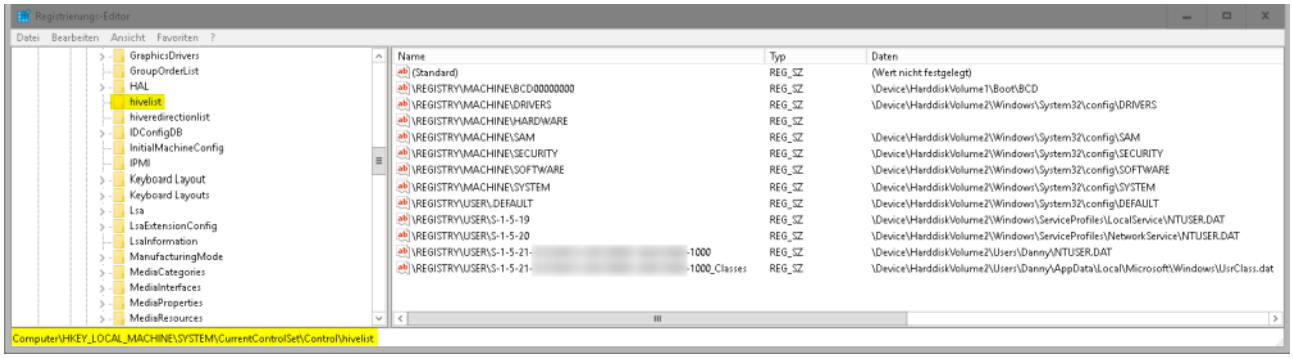
Änderungen in diesem Bereich wirken sich immer auf das gesamte System und alle Benutzer die sich an dem System anmelden aus.

Folgende Dateien spiegeln hierbei die einzelnen Schlüssel unter dem Hive wieder und finden sich im Windows-Installationsverzeichnis unter:

Registry Hive	Datei(en)
HKEY_LOCAL_MACHINE\Software	System32\config\Software
HKEY_LOCAL_MACHINE\SAM	System32\config\SAM
HKEY_LOCAL_MACHINE\Security	System32\config\Security
HKEY_LOCAL_MACHINE\System	System32\config\System
HKEY_LOCAL_MACHINE\Drivers	System32\config\Drivers

Tipp 1: Um eine Zuordnung aller Hives und zugehörigen Dateien zu erhalten, navigiert man zu dem Schlüssel

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist



HKEY_USERS

Dieser Hive umfasst alle benutzerspezifischen Konfigurationseinstellungen der Windows Registrierungsdatenbank und wird häufig schlicht mit HKU abgekürzt.

Änderungen in diesem Bereich wirken sich immer auf den speziellen Systembenutzeraccount aus.

Folgende Dateien spiegeln hierbei die einzelnen auf jedem Windows-System vorhandenen Schlüssel unter dem Hive wieder

Registry Hive	Datei(en)
HKU\.Default	System32\config\.Default
HKU\S-1-5-18	System32\config\.Default
HKU\S-1-5-19	%WINDIR%\ServiceProfiles\LocalService
HKU\S-1-5-20	%WINDIR%\ServiceProfiles\NetworkService

Die “kurzen” Benutzer-SIDs gehören zu lokalen, windows-eigenen “Dienstaccounts”.
S-1-5-18 = Local System
S-1-5-19 = NT Authority\LocalService
S-1-5-19 = NT Authority\NetworkService

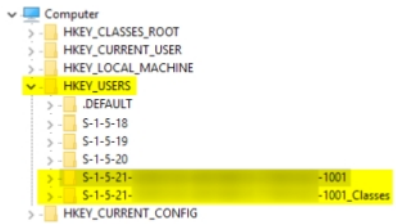
Nähere Infos zu bekannten Sicherheits-IDs in Windows Betriebssytemen findet sich hier:
https://support.microsoft.com/de-de/help/243330/well-known-security-identifiers-in-windows-operating-systems

Zudem wird unter HKU werden nach der Benutzeranmeldung an einem Windows System
die zu der Benutzeranmeldung gehörigen Benutzer-Registrierungsdateien “eingehangen”.

Sollten mehrere Benutzer gleichzeitig angemeldet sein (zum Beispiel über die Funktion “Benutzer wechseln” muss man die SID des jeweiligen Benutzeraccounts kennen oder über den Unterschlüssel

HKU\Benutzer-SID\VolatileEnvironment

und dessen Wert “Username” den entsprechenden Zweig herausfinden.



Zum Beispiel

Registry Hive	Datei(en)
S-1-5-21-123456-123456-123456-1001	%systemdrive%\Users\%username%\NTUSER.DAT
S-1-5-21-123456-123456-123456-1001_classes	%systemdrive%\Users\%username%\NTUSER.DAT

Die Datei, welche die benutzerspezifischen Einstellungen wiederspiegelt heißt ntuser.dat und liegt direkt im Wurzelverzeichnis des Benutzerprofils.

Der Zweig des aktuell angemeldeten Benutzers wird zudem, wie bereits unter LINK beschrieben, nach HKEY_CURRENT_USER “gespiegelt.